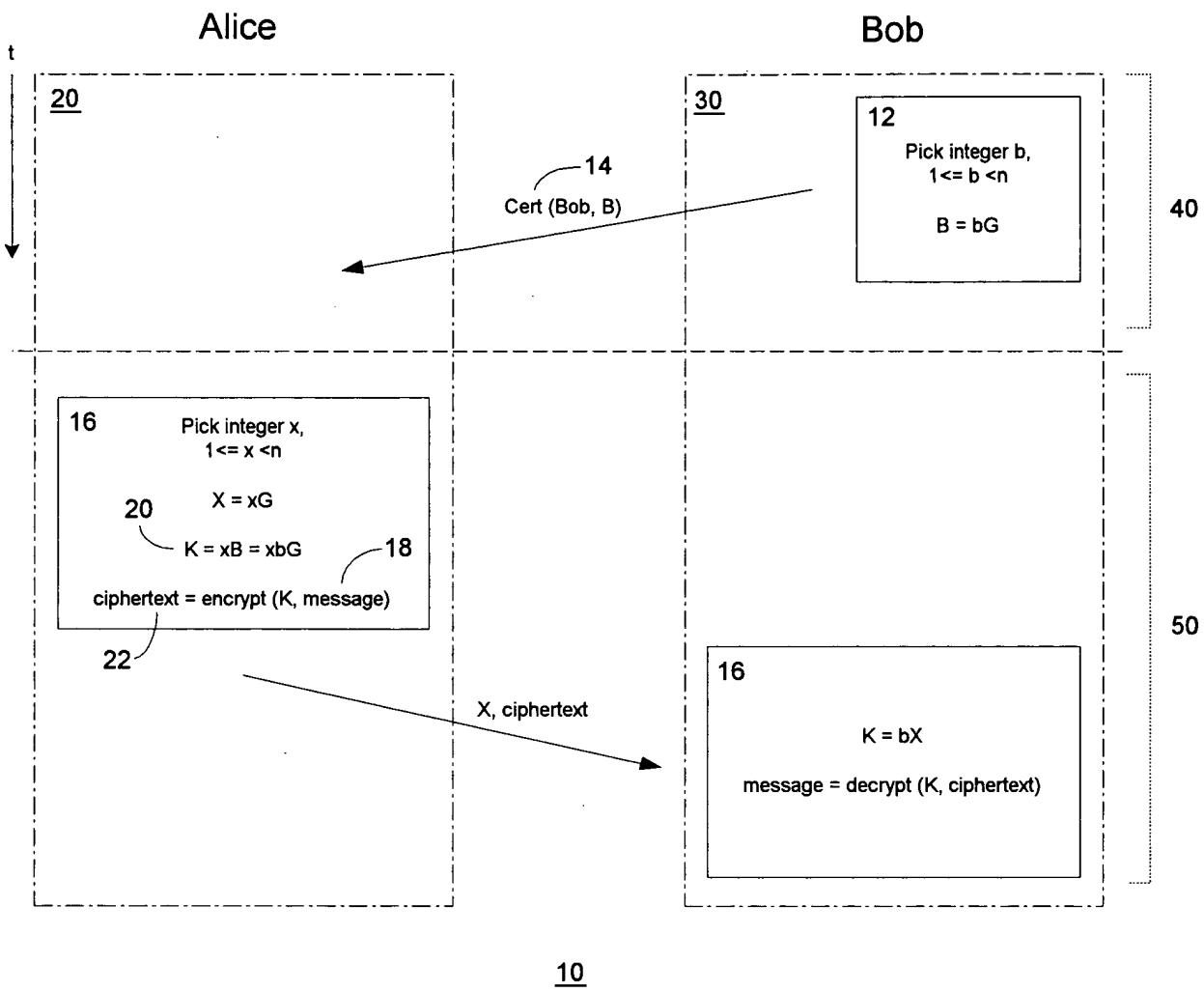

FIG 1 – PRIOR ART

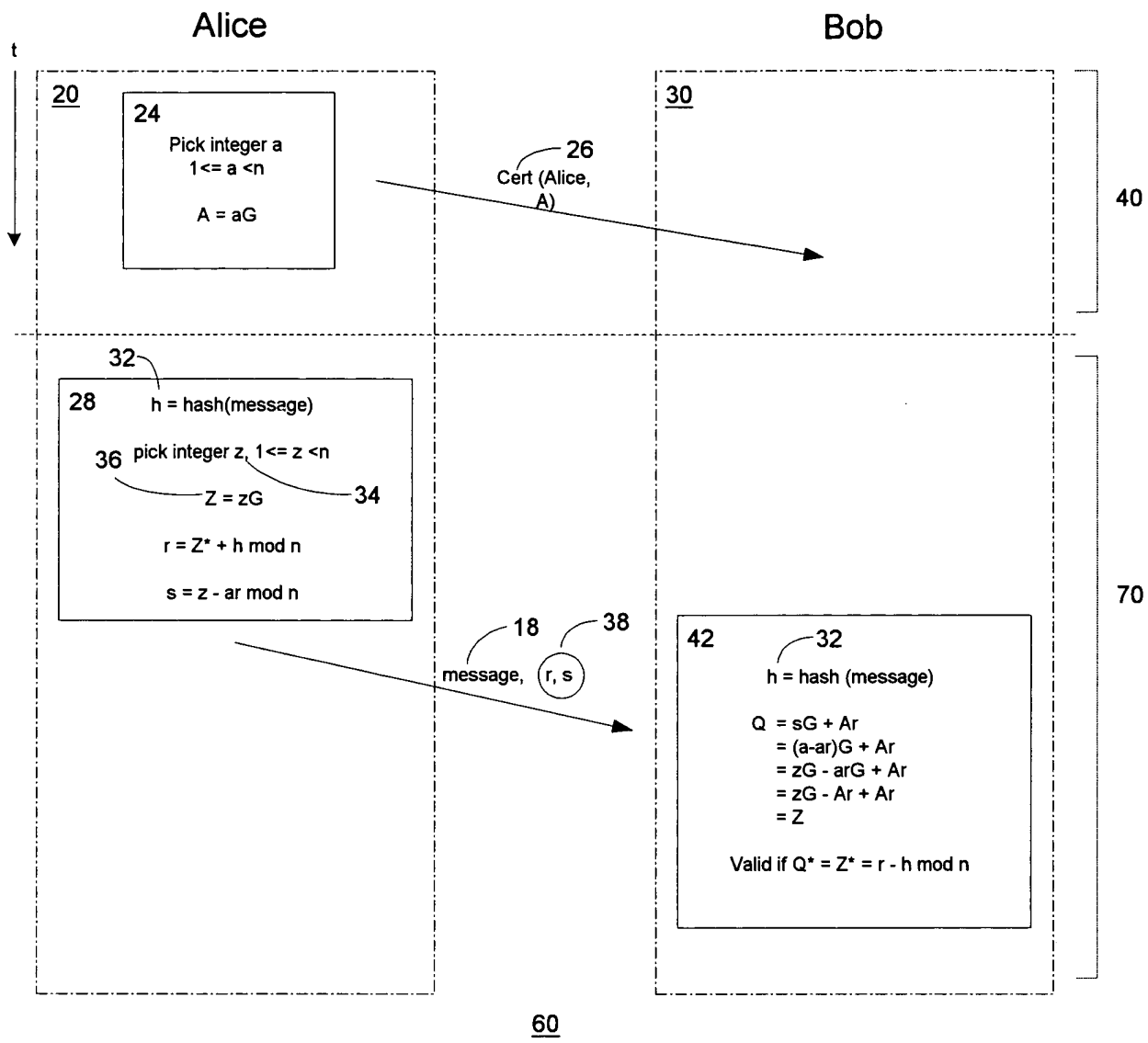

FIG. 2 – PRIOR ART

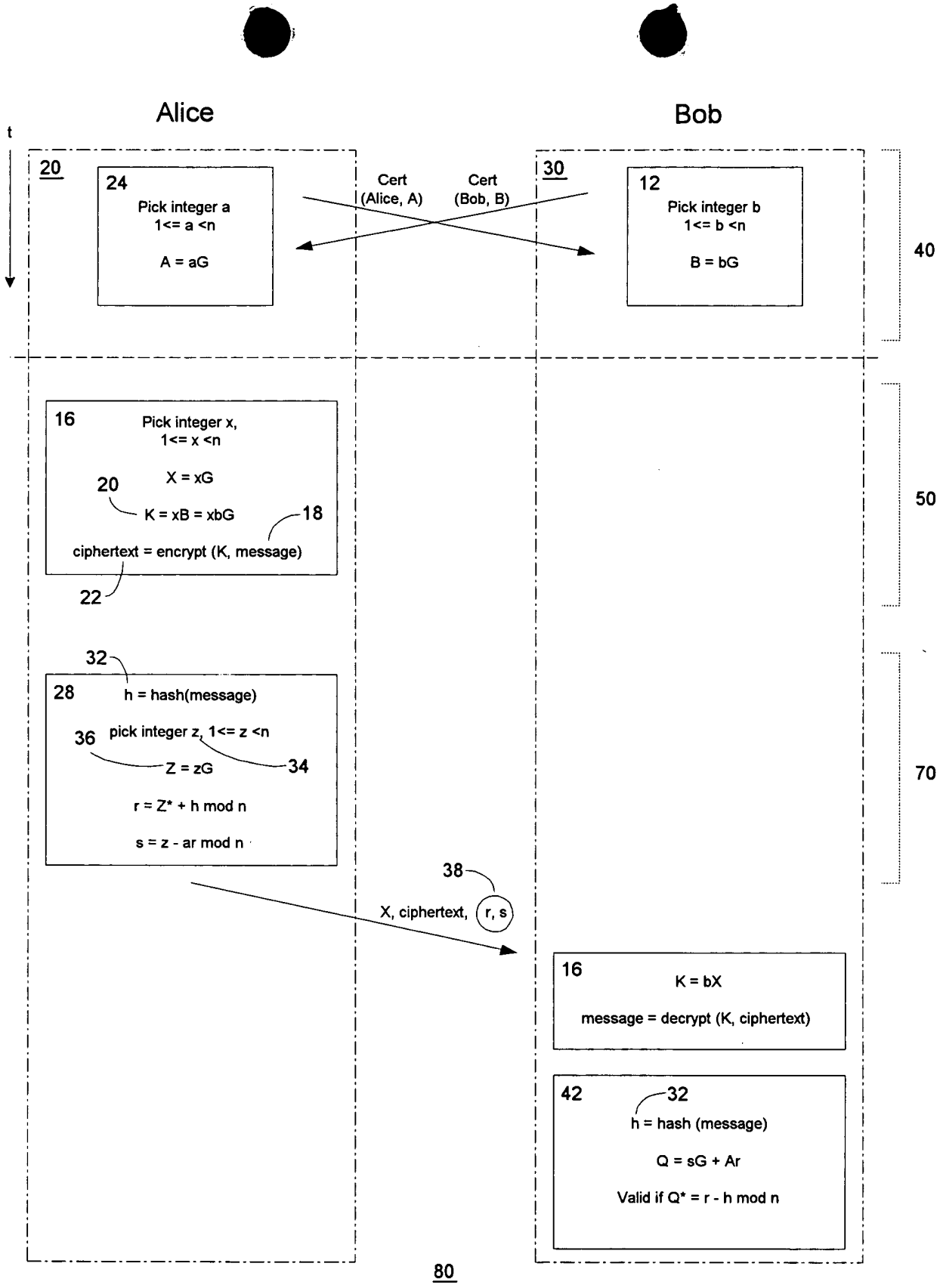
Alice
Bob
t
20
24
Pick integer a
1<= a <n
A = aG
Cert
(Alice, A)
Cert
(Bob, B)
30
12
Pick integer b
1<= b <n
B = bG
40
16
Pick integer x,
1<= x <n
X = xG
20
K = xB = xbG
18
ciphertext = encrypt (K, message)
22
50
32
28
h = hash(message)
pick integer z, 1<= z <n
36
Z = zG
34
r = Z* + h mod n
s = z - ar mod n
70
38
X, ciphertext,
r, s
16
K = bX
message = decrypt (K, ciphertext)
42
32
h = hash (message)
Q = sG + Ar
Valid if Q* = r - h mod n
80

FIG. 3 – PRIOR ART

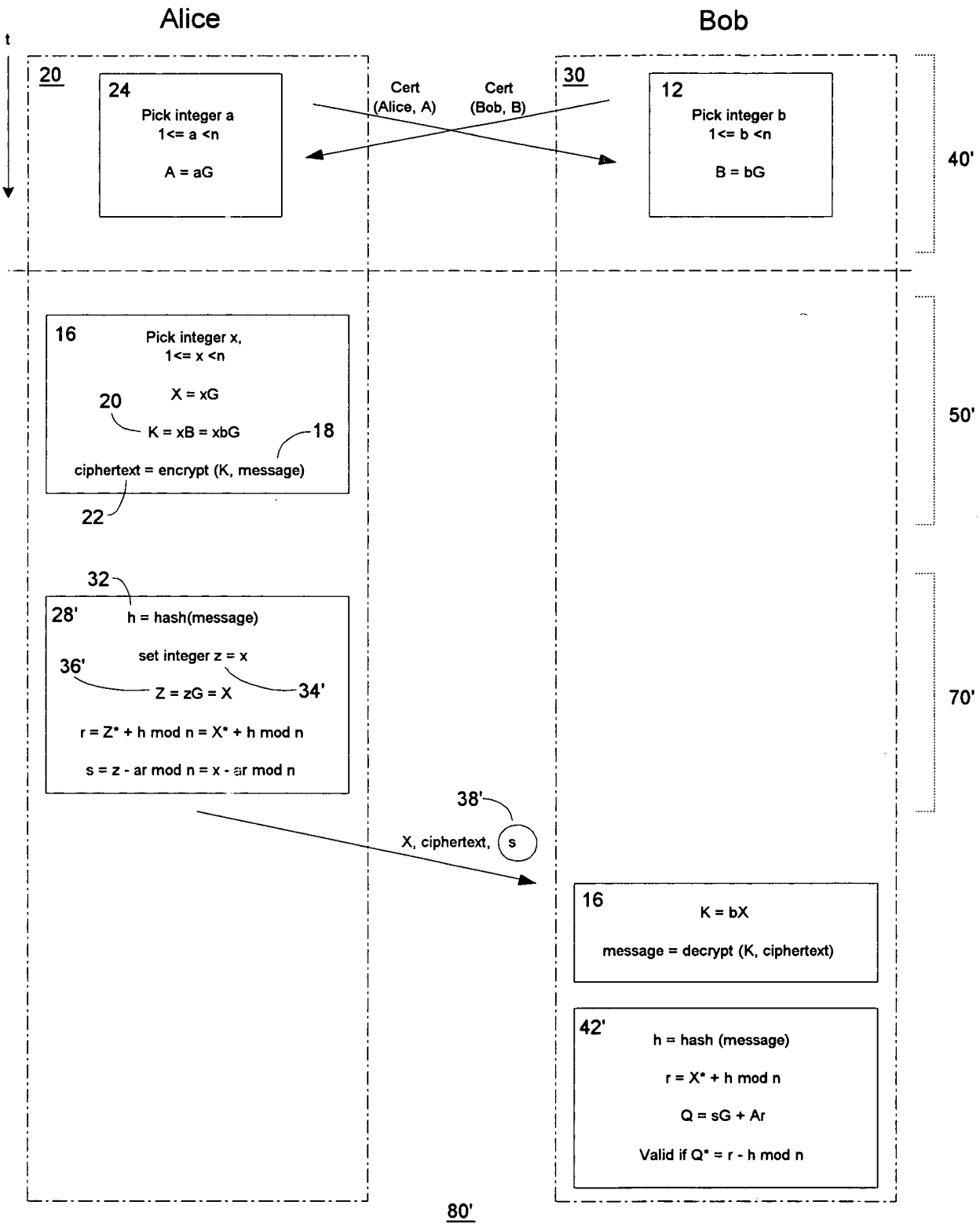

FIG. 4 - PRIOR ART

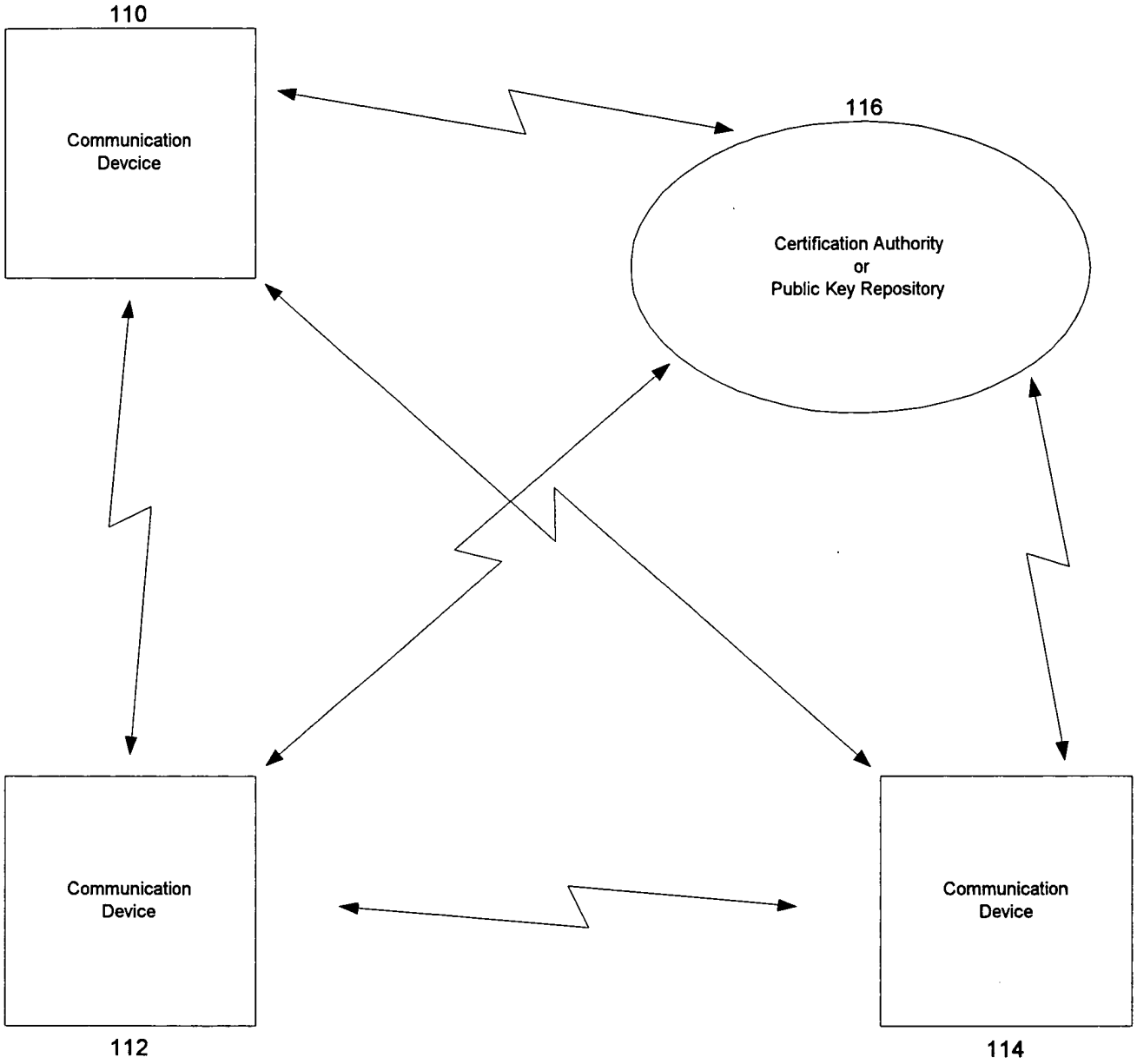

FIG. 5